The Claims

1. (Currently amended) A system supporting public key encryption, the system comprising:

a certifying authority;

a client device, coupled to the certifying authority, to,

generate a blinded certificate including a public key, and

transmit the blinded certificate to the certifying authority; and

wherein the certifying authority is to digitally sign the blinded certificate and encode security attributes of the client device into at least a portion of a key on which the digital signature is based.

2. (Original) A system as recited in claim 1, wherein the client device is further to receive the blinded certificate and generate a signed certificate by unblinding the signed blinded certificate.

3. (Original) A system as recited in claim 1, further comprising a content server coupled to provide electronic content to the client device

4. (Original) A system as recited in claim 3, wherein the client device is further to generate a signed certificate by unblinding the signed blinded certificate and to transfer the signed certificate to the content server, and wherein the content server is to check security attributes of the client device based on attributes encoded into the digital signature and to determine how to respond to the request based on the security attributes.

5. (Original) A system as recited in claim 4, wherein the content server can respond by doing one or more of the following: determining whether to deliver the requested content, determining what quality of content to deliver, or determining what additional security precautions to require of the client device.

6. (Original) A system as recited in claim 1, wherein the certifying authority is to digitally sign the blinded certificate according to a formula

$$(\text{blinded certificate})^{d} \bmod (n),$$

wherein d represents a private key of the certifying authority and wherein n is a product of two prime numbers that comprise the private key.

7. (Currently amended) A system ~~as recited in claim 6,~~ supporting public key encryption, the system comprising:

a certifying authority;

a client device, coupled to the certifying authority, to,

generate a blinded certificate including a public key, and

transmit the blinded certificate to the certifying authority;

wherein the certifying authority is to digitally sign the blinded certificate and encode security attributes of the client device into the digital signature;

wherein the certifying authority is to digitally sign the blinded certificate according to a formula

$$(\text{blinded certificate})^{d} \bmod (n),$$

wherein d represents a private key of the certifying authority and wherein n is a product of two prime numbers that comprise the private key; and

wherein the certifying authority is to encode a security attribute into the digital signature by:

representing the security attributes as a series of bits;

identifying, for each bit in the series that has a particular value, a corresponding integer; and

generating as the value d the product of the identified integers.

8. (Original) A system as recited in claim 7, wherein the certifying authority is further to generate another digital signature for the blinded certificate by:

additionally identifying, for each bit in the series that has another value, a corresponding integer; and

generating as the value d for the other digital signature the product of the additionally identified integers.

9. (Original) A method comprising:

receiving, from a client, a current certificate and a request to sign a new certificate;

determining attributes of the client based on the current certificate;

selecting, in accordance with public key cryptography, a public/private key pair that is based at least in part on the attributes of the client; and

digitally signing the new certificate using the selected private key.

10. (Original) A method as recited in claim 9, wherein the attributes are security attributes of the client.

11. (Currently amended) A method as recited in claim 9, wherein the new certificate is a blinded certificate.

12. (Currently amended) A method as recited in claim 9, further comprising determining additional information to encode into the digital signature, and wherein the selecting further comprises selecting the public/private key pair based on the attributes of the client and the additional information.

13. (Currently amended) A method as recited in claim 9, wherein the selecting comprises determining a bit pattern that corresponds to the security attributes of the client, and identifying a public/private key pair that corresponds to the bit pattern.

14. (Original) A method as recited in claim 9, wherein the digitally signing comprises calculating a value of a formula

$$(\text{blinded certificate})^{d} \bmod (n),$$

wherein d represents a private key of a device performing the digital signing and wherein n is a product of two prime numbers that comprise the private key.

15. (Currently amended) A method ~~as recited in claim 14,~~ comprising:

receiving, from a client, a current certificate and a request to sign a new certificate;

determining attributes of the client based on the current certificate;

selecting, in accordance with public key cryptography, a public/private key pair that is based at least in part on the attributes of the client;

digitally signing the new certificate using the selected private key;

wherein the digitally signing comprises calculating a value of a formula

$$(\text{blinded certificate})^{d} \bmod (n),$$

wherein d represents a private key of a device performing the digital signing and wherein n is a product of two prime numbers that comprise the private key; and

wherein the selecting comprises:

representing the attributes as a series of bits;

identifying, for each bit in the series that has a particular value, a corresponding integer; and

generating as the value d the product of the identified integers.

16. (Original) A method as recited in claim 15, further comprising generating another digital signature for the blinded certificate by:

additionally identifying, for each bit in the series that has another value, a corresponding integer; and

generating as the value *d* for the other digital signature the product of the additionally identified integers.

17. (Canceled).

18. (Currently amended) An apparatus to digitally sign electronic information, the apparatus comprising:

a connection module to establish a secure connection with a client device;

a signature module to receive electronic information from the client device and digitally sign the electronic information, encoding attributes of the client device into the digital signature by basing the digital signature on at least a portion of a key in which the attributes are encoded.

19. (Original) An apparatus as recited in claim 18, wherein the attributes are security attributes of the client device.

20. (Original) An apparatus as recited in claim 18, further comprising a certificate archive that stores currently valid certificates issued by the apparatus, and wherein the apparatus is further to receive a public key, check whether the certificate archive stores a currently valid certificate corresponding to the public key, and respond to the request based on the results of the checking.

21. (Canceled).

22. (Currently amended) A method as recited in claim 23~~21~~, wherein the determining how to respond comprises one or more of: determining what quality level of content to provide, determining what type of payment to require, and determining what additional security precautions are required on the part of the client.

23. (Currently amended) A method ~~as recited in claim 21,~~ comprising:

receiving, from a client, a request for electronic content;

checking, based on information encoded in a digital signature of at least a portion of the request, whether the client has a set of claimed security attributes;

determining how to respond to the request based on the checking; and

wherein the checking comprises determining a public key based on the set of claimed security attributes, and using the public key to verify the digital signature.

24. (Currently amended) A method as recited in claim 23~~21~~, wherein the checking further comprises:

representing the set of claimed security attributes as a series of bits; and

generating [[a]] the public key ~~for a certifying authority~~ using the series of bits~~; and~~

~~using the public key to verify the digital signature~~.

25. (Currently amended) A method ~~as recited in claim 24,~~ comprising:

receiving, from a client, a request for electronic content;

checking, based on information encoded in a digital signature of at least a portion of the request, whether the client has a set of claimed security attributes;

determining how to respond to the request based on the checking;

wherein the checking comprises:

representing the set of claimed security attributes as a series of bits;

generating a public key for a certifying authority using the series of bits; and

using the public key to verify the digital signature; and

wherein the generating comprises:

identifying, for each bit in the series that has a particular value, a corresponding integer; and

generating as the public key the product of the identified integers.

26. (Canceled).

27. (Currently amended) A method comprising:

generating a public/private key pair for use in public key cryptography;

creating a certificate including the public key;

transmitting the certificate to a certificate archive; ~~and~~

receiving, from the certificate archive, an indication of whether the certificate is currently valid; and

repeating the generating, creating, transmitting, and receiving for additional certificates until an indication that one of the certificates is currently valid is received.

28. (Currently amended) One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 27 ~~28~~.

29. (Original) A method for recovering from a device failure in a public key encryption system, the method comprising the following acts:

(a) generating a public/private key pair using a fixed algorithm and a fixed seed value;

(b) creating a certificate incorporating the public key;

(c) querying a certificate archive as to whether the certificate is valid;

(d) if the certificate is not valid, then generating a new public/private key pair using the fixed algorithm and based on the public key;

(e) repeating acts (b) – (d) until a valid certificate is created.

30. (Original) One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 29.

31. (New) One or more computer-readable media containing a plurality of instructions that, when executed by one or more processors, causes the one or more processors to:

receive, from a client, a current certificate and a request to sign a new certificate;

determine attributes of the client based on the current certificate;

select, in accordance with public key cryptography, a public/private key pair that is based at least in part on the attributes of the client; and

digitally sign the new certificate using the selected private key.

32. (New) One or more computer-readable media as recited in claim 31, wherein the attributes are security attributes of the client.

33. (New) One or more computer-readable media as recited in claim 31, wherein the new certificate is a blinded certificate.

34. (New) One or more computer-readable media as recited in claim 31, wherein the instructions that cause the one or more processors to select the public/private key pair further cause the one or more processors to determine a bit pattern that corresponds to the security attributes of the client, and identify a public/private key pair that corresponds to the bit pattern.

35. (New) One or more computer-readable media containing a plurality of instructions that, when executed by one or more processors, causes the one or more processors to:

receive, from a client, a request for electronic content;

check, based on information encoded in a digital signature of at least a portion of the request, whether the client has a set of claimed security attributes by determining a public key based on the set of claimed security attributes and using the public key to verify the digital signature; and

determine how to respond to the request based on the checking.

36. (New) One or more computer-readable media as recited in claim 35, wherein the instructions that cause the one or more processors to check whether the client has a set of claimed security attributes further cause the one or more processors to represent the set of claimed security attributes as a series of bits and generate the public key using the series of bits.

37. (New) One or more computer-readable media as recited in claim 36, wherein the instructions that cause the one or more processors to generate the public key further cause the one or more processors to:

identify, for each bit in the series that has a particular value, a corresponding integer; and

generate as the public key the product of the identified integers.